



The University of Texas at El Paso
Information Security Office
Data Classification Standard

Contents

Purpose	3
Scope.....	3
Data Classification Standard	3
Category-I Data	4
Category-II Data	4
Category-III Data	5
How to Classify Your Data	5
Data Classification Examples.....	6
Disciplinary Actions.....	7
APPENDIX A.....	8
Extended List of Category – I Data	8
Patient Medical/Health Information (HIPAA)	8
Student Records (FERPA)	8
Donor/Alumni Information (UTS165, Texas Identity Theft Enforcement and Protection Act, HIPAA)	8
Research Information (Granting Agency Agreements, Other Institutional Review Board –IRB - Governance).....	9
Employee Information (UTS165, Texas Identity Theft Enforcement and Protection Act).....	9
Business/Vendor Data (Gramm-Leach-Bliley Act, Non-Disclosure agreement)	9
Other Institutional Data (Gramm-Leach-Bliley Act, Other Considerations)	9

Revision History

First Draft: February 6, 2008

Purpose

This Data Classification Standard¹ serves as a supplement to the [Information Security Policy Manual](#), which was drafted in response to [Texas Administrative Code 202](#) and [UT System UTS-165](#). Adherence to the standard will facilitate applying the appropriate security controls to university data.

The objective of this standard is to assist [data stewards](#), IT [owners](#) and [custodians](#) in the assessment of information systems to determine what level of security is required to protect data on the [systems](#) for which they are responsible. The standard divides data into three categories:

- Category I
- Category II
- Category III

This standard exists in addition to all other university policies and federal and state regulations governing the protection of the university's data. Compliance with this classification standard will not ensure that data will be properly secured. Instead, this standard should be integrated into a comprehensive information security plan.

Scope

All university data stored on university resources or other resources where university business occurs must be classified into one of the three categories. This applies to all faculty, staff, student employees, contractors, and vendors working with University of Texas at El Paso data. Based on the data classification you determine for your system, you are required to implement appropriate technical security measures to protect the data consistent with the university Minimum Security Standards. Category-I data has more stringent requirements than Categories II and III. All systems require some protective measures.

Note: Data that is personal to the operator of a system and stored on a university IT resource as a result of incidental personal use is not considered university data. University data stored on non-university IT resources must still be verifiably protected according to the respective university minimum security standards.

Data Classification Standard²

To classify your data, you must start by understanding what the classifications are. There are specific laws and regulations that govern some kinds of data. Additionally, there are situations where you must consider whether the confidentiality, integrity, or availability of the data is a factor. Finally, consider that you may be storing information on more than one system, such as moving data between computers by CD or flash drive, for example. If you rate only your primary computer as Category-I, but not your secondary computer or the transfer media, the secondary computer could put data at risk because it will not be well protected.

¹ Adapted from the "[Data Classification Guideline](#)"

(<http://www.utexas.edu/its/policies/opsmanual/dataclassification.php>), with permission from ITS, The University of Texas at Austin, Austin, Texas 78710-1110

² Portions adapted by UT Austin from "Classification of Data"

(http://www.stanford.edu/group/security/classification/classification_of_data.html), with permission from Stanford University, Stanford, California 94305-4102

Category-I Data

University data protected specifically by federal or state law or University of Texas rules and regulations (e.g., HIPAA; FERPA; Sarbanes-Oxley, Gramm-Leach-Bliley; the Texas Identity Theft Enforcement and Protection Act; University of Texas System Business Procedure Memoranda; specific donor and employee data). University data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to contractual agreements requiring confidentiality, integrity, or availability considerations (e.g., Non Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc.) Any research data that has financial value to the University may be raised to this category. Please see the [extended Category-I data classification examples](#) in Appendix A for more examples of data protected under this classification.

Examples of How Data Can Be Lost	Impact of Category-I Data Loss
<ul style="list-style-type: none"> • Laptop or other data storage system stolen from car. • Research Assistant accesses system after leaving research project because passwords aren't changed. • Unauthorized visitor walks into unlocked lab and steals equipment or accesses unsecured computer. • Unsecured application on a networked computer is hacked and data stolen. 	<ul style="list-style-type: none"> • Long-term loss of research funding from granting agencies. • Long-term loss of reputation. Published research called into question because data is unreliable. • Unauthorized tampering of research data. • Increase in regulatory requirements. Long-term loss of critical campus or departmental service. • Individuals put at risk for identity theft.

Protect your Category-I data by applying the appropriate Minimum Security Standards.

Category-II Data

University data not otherwise identified as Category-I data, but which are releasable in accordance with the Texas Public Information Act (e.g., contents of specific e-mail, date of birth, salary, etc.) Such data must be appropriately protected to ensure a controlled and lawful release.

Examples of How Data Can Be Lost	Impact of Category-II Data Loss
<p>In addition to the above scenarios...</p> <ul style="list-style-type: none"> • Staff member wanting to be helpful releases information they are not authorized to share. 	<ul style="list-style-type: none"> • Short-term loss of reputation. • Short-term loss of research funding. • Short-term loss of critical departmental service. • Unauthorized tampering of research data. • Individuals put at risk for identity theft.

Protect your Category-II data by applying the appropriate Minimum Security Standards.

Category-III Data

University data not otherwise identified as Category-I or Category-II data (e.g., publicly available). Such data have no requirement for confidentiality, integrity, or availability.

Examples of How Data Can Be Lost	Impact of Category-III Data Loss
See the above scenarios.	Loss of use of personal workstation or laptop. Loss of personal data with no impact to the university.

Protect your Category-III data by applying the appropriate Minimum Security Standards.

How to Classify Your Data

If you are evaluating data you are responsible for and it doesn't clearly fall under the laws and regulations listed in the definition, you can apply the Confidentiality, Integrity, and Availability (CIA) criteria. (Most of the legal and regulatory requirements are driven by confidentiality and integrity concerns.)

- **Confidentiality:** The need to strictly limit access to data to protect the university and individuals from loss.
- **Integrity:** Data must be accurate, and users must be able to trust its accuracy.
- **Availability:** Data must be accessible to authorized persons, entities, or devices.

To determine the level of protections applied to a system, base your classification on the most *confidential* data stored in the system. A positive response to the highest category in **ANY** row is sufficient to place the data into that respective category. Even if the system stores data that could be made available in response to an open records request or information that is public, the entire system must still be protected based on the most confidential data.

Data Classification Weighting

	Category I	Category II	Category III
Need for Confidentiality	Required (High)	Recommended (Medium)	Optional (Low)
	AND/OR	AND/OR	AND/OR
Need for Integrity	Required (High)	Recommended (Medium)	Optional (Low)
	AND/OR	AND/OR	AND/OR
Need for Availability	Required (High)	Recommended (Medium)	Optional (Low)

Data Classification Examples

This section illustrates how the Information Security Office classifies some familiar data using the CIA (Confidentiality, Integrity, Availability) criteria.

Category-I Data: Student Information System

Student Information System is considered Category-I data because it dictates a high level of uptime.

- **Need for Confidentiality is required (high)**
- **Need for Integrity is required (high)**
- Need for Availability is recommended (medium)

Since two of the CIA conditions are required (high), in this case availability, Student Information Systems is considered Category-I data.

Category-I Data: Digital Research Data with a Funding Agency Agreement

Digital research data is required to be confidential (high) due to various factors, including human subject data, requirements of granting or funding agency agreements, etc. Integrity of the research is required (high) because the data must be accurate and free from errors to be credible. Availability is recommended (medium), because The University of Texas at El Paso is not necessarily in any danger or in violation of any law if the data is unavailable for a period of time.

- **Need for Confidentiality is required (high)**
- **Need for Integrity is required (high)**
- Need for Availability is recommended (medium)

Category-II Data: Large Numbers of E-mail Addresses

University e-mail addresses are considered Category-II data. By law they are public information and are published in the university directory (unless restricted by individuals). However, the directory is not intended to be used to harvest e-mail addresses. People must submit open records requests to get e-mail addresses.

- Need for Confidentiality is optional (low)
- Need for Integrity is recommended (medium)
- Need for Availability is recommended (medium)

You may ask yourself why integrity is only recommended and not required. In this case, we are not talking about the source system that stores official e-mail addresses, but the release of that information.

Category-III Data: Professor's Blog

A blog is by its very nature designed to be shared with the world. The confidentiality requirement is therefore optional (low). If the contents of the blog are changed, there would be little to no impact on the ability of the department or the university to carry out their missions. The need for integrity is therefore optional (low). The need for availability is also optional (low) because, should the blog be

taken offline for a period of time, the only primary people affected would be the readers of the blog. The department and university should be able to carry on business as usual, while the blog was restored or recreated.

Summary of a professor's blog hosted on a departmental server:

- Need for Confidentiality is optional (low)
- Need for Integrity is optional (low)
- Need for Availability is optional (low)

Since at all of the CIA conditions are optional (low), a professor's blog hosted on a departmental server is considered Category-III data and should be protected using the required and recommended standards for Category-III data.

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTEP Information Resources access privileges, civil, and criminal prosecution. University of Texas at El Paso employees are required to comply with both institutional rules and regulations and applicable UT System rules and regulations. In addition to university and System rules and regulations, University of Texas at El Paso employees are required to comply with state laws and regulations.

APPENDIX A

Extended List of Category – I Data

Patient Medical/Health Information (HIPAA)

The following information is confidential:

- Social security number
- Patient names, street address, city, county, zip code, telephone / fax numbers
- Dates (except year) related to an individual, account / medical record numbers, health plan beneficiary numbers
- Personal vehicle information
- Certificate / license numbers, device IDs and serial numbers, e-mail, URLs, IP addresses
- Access device numbers (ISO number, building access code, etc.)
- Biometric identifiers and full face images
- Any other unique identifying number, characteristic, or code
- Payment Guarantor's information

Student Records (FERPA)

The following information is confidential. This applies to both enrolled and prospective student data.

- Social security number
- 800 number
- Grades (including test scores, assignments, and class grades)
- Student financials, credit cards, bank accounts, wire transfers, payment history, financial aid/grants, student bills
- Access device numbers (ISO number, building access code, etc.)
- Biometric identifiers

Note that for enrolled students, the following data may ordinarily be revealed by the university without student consent unless the student designates otherwise:

- Name, directory address and phone number, mailing address, secondary mailing or permanent address, residence assignment and room or apartment number, campus office address (for graduate students)
- Date of birth, place of birth
- Electronic mail address
- Specific semesters of registration at UTEP; UTEP degree(s) awarded and date(s); major(s), minor(s), and field(s); university degree honors
- Institution attended immediately prior to UTEP
- ID card photographs for university classroom use

Donor/Alumni Information (UTS165, Texas Identity Theft Enforcement and Protection Act, HIPAA)

The following information is confidential:

- Social security number
- Name
- Personal financial information
- Family information
- Medical information

- Credit card numbers, bank account numbers, amount / what donated
- Telephone / fax numbers, e-mail, URLs

Research Information (Granting Agency Agreements, Other Institutional Review Board –IRB - Governance)

The following information is confidential:

- Funding / sponsorship information
- Human subject information
- Sensitive digital research data

Employee Information (UTS165, Texas Identity Theft Enforcement and Protection Act)

There can be confusion over which rules apply when an employee is also a student. The rule of thumb is that the student rules apply when the employee is in a student job title.

The following employee information is confidential:

- Social security number
- Personal financial information, including non-UT income level and sources
- Insurance benefit information
- Access device numbers (ISO number, building access code, etc.)
- Biometric identifiers
- Family information, home address, and home phone number ***may be revealed unless restricted by the employee.***

Please note that public employee names, birth dates, salary, and performance review information that would be released under an open records request.

Business/Vendor Data (Gramm-Leach-Bliley Act, Non-Disclosure agreement)

The following information is confidential:

- Vendor social security number
- Credit card information
- Contract information (between UTEP and a third party)
- Access device numbers (ISO number, building access code, etc.)
- Biometric identifiers
- Certificate / license numbers, device IDs and serial numbers, e-mail, URLs, IP addresses

Other Institutional Data (Gramm-Leach-Bliley Act, Other Considerations)

The following information is confidential:

- Information pertaining to the Office of Institutional Relations and Legal Affairs
- Financial records
- Contracts
- Physical plant detail
- Credit card numbers
- Certain management information
- Critical infrastructure detail
- User account passwords